



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1459
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/867,648	05/31/2001	Nang Kon Kwan	6502.0345	7988

22852 7590 04/15/2004

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
1300 I STREET, NW
WASHINGTON, DC 20005

EXAMINER

PHAM, KHANH B

ART UNIT	PAPER NUMBER
----------	--------------

2177

DATE MAILED: 04/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/867,648

Applicant(s)

KWAN, NANG KON

Examiner

Khanh B. Pham

Art Unit

2177

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08 January 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-29 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-29 is/are rejected.
- 7) ☒ Claim(s) 12 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

Art Unit: 2177

DETAILED ACTION

Response to Amendment

1. The amendment filed January 8, 2004 has been entered. Claims 1-7, 9-10, 12-13, 15-21, 23, 25, 28, and 29 have been amended.

Claim Objections

2. Claim 12 is objected to because of the following informality: the meaning of the phrase: "returning a LDAP database query result indicating whether the digital certificate the database record is stored in the database" is unclear. Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. **Claims 1-13, 16-29 are rejected** under 35 U.S.C. 102(e) as being anticipated by Sinn (US 2002/0166049 A1), hereinafter "Sinn".

As per claims 1, 17, 29, Sinn discloses a method and a computer readable medium for validating digital certificates having a server (Fig. 52, element 2076), an Online Certificate Status Protocol responder (element 2072), a certificate authority (element 2084), and a certificate database (element 36) including records associated with digital certificates, comprising:

- "receiving at the OCSP responder an OCSP request associated with a digital certificate generated by the server" at [0393];
- "creating by the OCSP responder, a Lightweight Directory Access Protocol database query based on the received OCSP request" at [0119] and [0394];
- "sending by the OCSP responder the Lightweight Directory Access Protocol database query to the certificate database to determine whether the digital certificate is valid" at [0119];
- "receiving at the OCSP responder a database query result indicating whether the digital certificate matches a corresponding certificate entry stored in one of the certificate database records" at [0397].
- "determining, by the OCSP responder, the validity of the digital certificate based on the database query result" at [0394];
- "notify the server of the determined validity of the digital certificate." at [0399]

As per claims 2, 18, Sinn teaches the method and the computer readable medium of claims 1, 17, wherein “the Lightweight Directory Access Protocol database query includes an instruction to return a selected portion of a database record” at [0128]-[0129].

As per claims 3, 19, Sinn teaches the method and the computer readable medium of claims 1, 17, wherein the method further comprises:

- “sending an indication of a new digital certificate from the certificate authority to the certificate database upon issuance of the new digital certificate” at [0374] ;
- “receiving, by the certificate database, from the certificate authority, an indication of the new digital certificate; and creating a certificate database record reflecting an identity of the new digital certificate” at [0374].

As per claims 4, 20, Sinn teaches the method and computer readable medium of claims 1, 17, wherein the method further comprises:

- “sending an indication of a revoked digital certificate from the certificate authority to the certificate database upon revocation of the revoked digital certificate” at [0382];
- “receiving, by the certificate database, from the certificate authority, the indication of revocation of the revoked digital certificate” at [0383];
- “removing a certificate database record associated with the revoked digital certificate from the certificate database” at [0384] .

As per claims 5, 21, Sinn teaches a method and a computer readable medium in a data processing system for validating digital certificates, the data processing system having a certificate authority and a directory server having a database, the method performed by the directory server comprising:

- “receiving, a Lightweight Directory Access Protocol query based on an online certificate status protocol request indicating a requested digital certificate” at [0119] and [0393];
- “searching the database for a database record reflecting an identity of the requested digital certificate” at [0393];
- “and returning an indication of the database record when the database record reflecting the requested digital certificate is found to indicate validity of the requested digital certificate” at [0393];
- “whereby the indication of the database record includes meta-data reflecting the validity of the requested digital certificate.” at [0394].

As per claims 6, 22, Sinn teaches the method and the computer readable medium of claims 5, 21, further comprising the step of:

- “sending an indication of a new digital certificate from the certificate authority to the database upon issuance of the new digital certificate” at [0374];
- “receiving, by the database from the certificate authority, an indication of the new digital certificate upon issuance of the new digital certificate” at [0375];

- “and storing a database record reflecting an identity of the new digital certificate” at [0375].

As per claims 7, 23, Sinn teaches a method and the computer readable medium for validating digital certificates without certification revocation lists, comprising:

- “receiving, from a server, an online certificate status protocol request associated with a digital certificate” at [0393];
- “creating a database query based on the received request; sending the database query to a database to determine whether the digital certificate is valid” at [0393];
- “receiving a database query result indicating that the digital certificate matches an entry in the database” at [0394];
- “providing the database query result to the server that determines that the digital certificates is valid based on the indication of the matching database entry” at [0393];
- “sending, from the server to a digital certificate requesting entity, an indication that the digital certificate is valid” at [0399].

As per claims 8, 24, Sinn teaches the method and the computer readable medium of claims 7, 23, wherein “the database query is a Lightweight Directory Access Protocol database query” at [0128].

As per claims 9, 25, Sinn teaches a method and a computer readable medium for validating digital certificates without certification revocation lists [0010], the data processing system having a requesting entity that requests a status of a digital certificate from a remote computing entity (Fig. 52, element 40), a certificate authority (element 2084), and a database (element 36), the method comprising:

- “receiving, by the database, a query based on an online certificate status protocol request indicating a requested digital certificate” at [0393],
- “wherein the request is generated by the remote computing entity based on a status request received from the requesting entity” at [0399];
- “searching the database for a database record reflecting an identity of the requested digital certificate” at [0394];
- “returning a first indication of the database record when the database record reflecting the requested digital certificate is found in the database; ” at [0393].
- “returning a second indication of the database record when the database record reflecting the requested digital certificate is not found in the database” at [0393]
- “wherein the remote computing entity determines that the digital certificate is valid when the first indication is returned and determines that the digital certificate is invalid when the second indication is returned” at [0393];

- “sending, from the remote computing entity to the requesting entity, a third indication reflecting the invalidity or validity of the digital certificate” at [0399]

As per claims 10, 26, Sinn teaches the method and the computer readable medium of claims 9, 25, further comprising:

- “sending an indication of the new digital certificate from the certificate authority to the database upon issuance of the new digital certificate; receiving, by the database from the certificate authority, an indication of a new digital certificate upon issuance of the new digital certificate; and storing a database record reflecting an identity of the new digital certificate” at [0374]-[0375].

As per claims 11, 27, Sinn teaches the method and the computer readable medium of claims 9, 25, wherein “the received query is a Lightweight Directory Access Protocol query” at [0128].

As per claims 12, 28, Sinn teaches a method and a computer readable medium in a data processing system for validating digital certificates without certification revocation lists, the data processing system having a client, a server, a responder, a certificate authority, and a database storing records of valid digital certificates of the certificate authority (see Fig. 52), the method comprising:

- “generating, by the client, a request for a transaction, the request including a digital certificate identifying the client; receiving the client request by the server” at [0399];
- “creating, by the server, an online certificate status protocol request based on the associated digital certificate identifying the client; sending, by the server, an online certificate status protocol request to the responder;” at [0393];
- “receiving, by the OCSP responder, the online certificate status protocol request associated with the digital certificate; creating, by the responder, a Lightweight Directory Access Protocol database query based on the received online certificate status protocol request” at [0128] and [0394];
- “sending, by the responder, the Lightweight Directory Access Protocol database query to the database to determine whether the digital certificate is valid” at [0128]-[0129] and [0393];
- “searching the database for a database record identifying the digital certificate associated with the online certificate status protocol request; returning a LDAP database query result indicating whether the digital certificate the database record is stored in the database;” at [0393]-[0394].
- “sending, by the responder, a validity indication whether the digital certificate is valid based on the query result to the server” [0393];

- “sending, by the server to the client, an indication of whether the transaction is authorized based on the validity indication” at [0399].

As per claim 13, Sinn teaches a data processing system for answering online certificate status requests without certificate revocation lists, comprising:

- a memory having program instructions; a processor configured to execute the program instructions to receive from a server an online certificate status protocol request associated with a digital certificate” at [0393],
- “create a database query based on the received request, send the Lightweight Directory Access Protocol database query to a database to determine whether the digital certificate is valid” at [0128],
- “receive a Lightweight Directory Access Protocol database query result from the database indicating whether the digital certificate matches a corresponding entry stored in a database one of the certificate database record” at [0393],
- “determining the validity of the digital certificate based on the database query result, and notify the server of the determined validity of the digital certificate.” at [0394].

As per claim 16, Sinn teaches a data processing system for answering online certificate status requests without certificate revocation lists, comprising:

- “a client computer configured to send a request for a transaction, the request including a digital certificate identifying the client” at [0399];

- “a server computer configured to receive the client request, create an online certificate status protocol request based on the associated digital certificate identifying the client” at [0393];
- “and send the online certificate status protocol request; an OCSP responder configured to receive the online certificate status protocol request associated with the digital certificate” at [0393];
- “create a Lightweight Directory Access Protocol database query based on the received online certificate status protocol request, and send the Lightweight Directory Access Protocol database query to determine whether the digital certificate is valid” at [0393] and [0128];
- “a database storing records of valid certificates of the certificate authority and configured to search for a database record identifying the digital certificate associated with the online certificate status protocol request” at [0393];
- “return an LDAP database query result indicating whether the digital certificate matches one of the records stored in the database” at [0393] .
- “wherein the OCSP responder determines that the digital certificate is valid when it receives an LDAP database query result reflecting that the digital certificate matches one of the database records” at [0394].

5. **Claims 14-15 are rejected** under 35 U.S.C. 102(a) as being anticipated by Wohlmacher ("Digital Certificates: a Survey of Revocation Methods"), hereinafter referred to as "Wohlmacher".

As per claim 14, Wohlmacher teaches a data processing system for answering online certificate status requests without certificate revocation lists, comprising:

- "a first computer having: a memory having program instructions; a processor configured to execute the program instructions to receive an online certificate status protocol request associated with a digital certificate" at page 114, Col. 1, 2nd paragraph;
- "create a database query based on the received request, send the database query to determine whether the digital certificate is valid, and receive a database query result indicating whether the digital certificate is valid" at page 114, Col. 1, 2nd paragraph;
- "and a second computer representing a directory server having: a database storing database records indicating digital certificates; a memory having program instructions; a processor configured to execute the program instructions to receive, from a certificate authority, an indication of a new digital certificate upon issuance of the new digital certificate, store a database record reflecting an identity of the new digital certificate, receive the database query based on the online certificate status protocol request from the first computer, search the database for a database record reflecting an identity of the requested digital

certificate; and return an indication of the database record to the first computer when the database record reflecting the requested digital certificate is found to indicate validity of the requested digital certificate” at page 113, Col. 1, 2nd paragraph.

As per claim 15, Wohlmacher teaches the data processing system of claim 14, wherein “the database query is an LDAP query” at page 114, Col. 1, 3rd paragraph.

Response to Arguments

6. Applicant's arguments with respect to claims 1-13, 15-29 have been considered but are moot in view of the new ground(s) of rejection.

7. Applicant's arguments filed with respect to claim 14 have been fully considered but they are not persuasive. The examiner respectfully traverses applicant's arguments.

Applicant argued that Wohlmacher does not teach “a processor configured to search a database for a database record reflecting an identify of the requested digital certificates; and return an indication of the database record to the first computer when the database record reflecting the requested digital certificate is found to indicate validity of the requested digital certificate”. On the contrary, Wohlmacher teaches: “the client generates a so call OCSP request that primary contains one or even more identifiers of certificates queried, i.e., their serial number together with other data. Then, the (optionally signed) request is send to the server. The server receiving the OCSP request creates an OCSP response”, and “The OCSP response is send to the requesting client of the user who then analyses the data” at page 114, Col. 1.

Wohlmacher also teaches the server "representing a directory" and the Certificate Authority submits certificate information such as serial numbers, expiration data, reason of revocation at page 113, Col. 1. Therefore, Wohlmacher's directory is similar to applicant database, which are used for storage and retrieval of Certificate record.

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. If a copy of a provisional application listed on the bottom portion of the accompanying Notice of References Cited (PTO-892) form is not included with this Office action and the PTO-892 has been annotated to indicate that the copy was not readily available, it is because the copy could not be readily obtained when the Office action was mailed. Should applicant desire a copy of such a provisional application,

Art Unit: 2177

applicant should promptly request the copy from the Office of Public Records (OPR) in accordance with 37 CFR 1.14(a)(1)(iv), paying the required fee under 37 CFR 1.19(b)(1). If a copy is ordered from OPR, the shortened statutory period for reply to this Office action will not be reset under MPEP § 710.06 unless applicant can demonstrate a substantial delay by the Office in fulfilling the order for the copy of the provisional application. Where the applicant has been notified on the PTO-892 that a copy of the provisional application is not readily available, the provision of MPEP § 707.05(a) that a copy of the cited reference will be automatically furnished without charge will not apply.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Khanh B. Pham whose telephone number is (703) 308-7299. The examiner can normally be reached on Monday through Friday 7:30am to 4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John E Breene can be reached on (703) 305-9790. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Khanh B. Pham
Examiner
Art Unit 2177

KBP
March 18, 2004


JEAN R. HOMERE
PRIMARY EXAMINER